UNITED STATES TRANSPORTATION COMMAND
Scott Air Force Base, Illinois 62225-5357

USTRANSCOM INSTRUCTION 33-35
20 October 2003

Communications and Information

UNITED STATES TRANSPORTATION COMMAND (USTRANSCOM) PRIVACY ACT (PA) PROGRAM

BY ORDER OF THE DEPUTY COMMANDER
COMPLIANCE WITH THIS PUBLICATION IS MANDATORY
NOTICE: This publication is available electronically in the USTRANSCOM electronic Library.

OPR: TCCS-IM
Approved by: TCCS-IM (Mary E. Wilson)
Supersedes: USTRANSCOMI 33-35, 17 Sep 01
Pages: 31
Distribution: Electronic Publishing

This instruction establishes policies, procedures, and responsibilities for implementing the United States Transportation Command (USTRANSCOM) Privacy Act (PA) Program governing collecting, safeguarding, maintaining, using, accessing, amending, and disseminating personal information maintained by USTRANSCOM systems of records. This instruction is applicable to all personnel assigned to USTRANSCOM. The components will follow their Service instructions for information maintained by systems of records generated within their area of responsibility. This instruction implements Federal law, Department of Defense (DOD), and Air Force (AF) regulations listed in Attachment 1, and contains additional instructions and guidance affecting the USTRANSCOM Privacy Act Program. Use in conjunction with those publications. This instruction does not apply to Freedom of Information Act (FOIA) requests, information from systems of records controlled by the Office of Personnel Management (although maintained by a DOD component), or requests for personal information from the General Accounting Office. This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by Title 10, United States Code, Section 8013. System of Records Notice F033 AF B, Privacy Act Request File, applies. Maintain and dispose of records created as a result of processes prescribed by this instruction in accordance with Chairman Joint Chiefs of Staff Manual (CJCSM) 5760.01, Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures and Volume II, Disposition Schedule. A USTRANSCOM member can file a civil suit against their respective Service for failure to comply with the Privacy Act; for example, willfully maintaining a system of records that doesn't meet the public notice requirements; disclosing information from a system of records to someone not entitled to the information, or obtaining records under false pretenses.

SUMMARY OF REVISIONS

Overall, generally updates the text. This revision prescribes Air Force Visual Aid 33-276, Privacy Act Label, as optional; adds the Electronic Government Act of 2002 requirement for a Privacy Impact Assessment for all information systems that are new or have major changes; adds Privacy Act warning language to use on information systems subject to the Privacy Act; includes guidance on sending personal information via electronic mail; adds procedures on complaints;

provides guidance on recall rosters, social rosters, consent statements, and placing information on shared drives; and provides guidance on systems of records operated by a contractor. (*NOTE: Since this instruction has been revised in its entirety, asterisks will not be used to identify revised material.)*

1. REFERENCES AND SUPPORTING INFORMATION. References, abbreviations, acronyms, and terms used in this instruction are listed in Attachment 1.

2. POLICY. The Privacy Act of 1974 and this instruction apply to information contained in USTRANSCOM Privacy Act systems of records.

2.1. An official system of records is authorized by law or Executive Order and required to carry out a USTRANSCOM mission or function.

2.2. USTRANSCOM does not:

2.2.1. Keep records on how a person exercises First Amendment rights. *Exceptions* are when USTRANSCOM has the permission of that individual or is authorized by federal statute, or the information pertains to an authorized law enforcement activity.

2.2.2. Penalize or harass an individual for exercising rights guaranteed under the Privacy Act and will give reasonable aid to individuals exercising their rights.

2.3. USTRANSCOM staff members will:

2.3.1. Keep paper and electronic records containing personal information and retrieved by name or personal identifier only in approved systems of records published in the Federal Register.

2.3.2. Collect, maintain, and use information in such systems only to support programs authorized by law or Executive Order.

2.3.3. Safeguard records included in the systems and keep them the minimum time required.

2.3.4. Keep the records timely, accurate, complete, and relevant.

2.3.5. Amend and correct records on request.

2.3.6. Let individuals review and receive copies of their own records unless an exemption for the system exists or records were created in anticipation of a civil action or proceeding.

2.3.7. Provide a review of decisions that deny individuals access to or amendment of their records.

2.4. Personal Notes. The Privacy Act does not apply to personal notes on individuals for use as memory aids to supervise or perform other official functions that are not shared with others and no USTRANSCOM directive requires maintenance.

2.5. Systems of Records Operated By a Contractor. Contractors who are required to operate or maintain a Privacy Act system of records by contract are considered employees of USTRANSCOM during the performance of the contract. The record system affected is maintained by USTRANSCOM and is subject to this instruction. Offices who have contractors operating or maintaining such record systems must ensure the contract contains the proper PA clauses, and identify the record system number. Records maintained by the contractor for the management of contractor employees are not subject to the PA.

3. RESPONSIBILITIES:

3.1. Chief of Staff, Information Management (TCCS-IM), Information Management Communications and Records Management (TCCS-IMR) will serve as the USTRANSCOM Privacy Act Officer. The Privacy Act Officer will manage the program; guide and train; review the program at regular intervals; review all publications and forms for compliance with this instruction; review proposed new, altered, and amended systems notices; review/resolve complaints or allegations of Privacy Act violations; review annually contracts for systems of records operated or maintained by a contractor; answer general Privacy Act questions and correspondence; and staff denial recommendations.

3.2. Systems of Records Managers are the officials who are responsible for managing a system of records, including policies and procedures to operate and safeguard it. Systems Managers will decide the need for and content of systems; manage and safeguard the system; train personnel on PA requirements; protect records from unauthorized disclosure, alteration, or destruction; prepare systems notices and reports; answer PA requests; investigate complaints or allegations, establish and review the facts, interview individuals as needed, determine validity of the complaint, and take appropriate corrective action; keep records of disclosures; and evaluate the systems annually.

3.3. Service Element Commanders, Directors, Command Support Group (CSG) Chiefs, Functional Managers, and Supervisors within USTRANSCOM are responsible for ensuring PA data under their control comply with the following:

3.3.1. USTRANSCOM Force Protection (TCFP) may request information from other agencies for law enforcement under Title 5 United States Code, Section 552a(b)(7). TCFP must indicate in writing the specific part of the record desired and identify the law enforcement activity requesting the record.

3.3.2. Record promises of confidentiality to exempt from disclosure any "confidential" information under Title 5 United States Code 552a, Subsection (k)(2), (k)(5), or (k)(7) of the Privacy Act.

3.3.3. Collect personal information directly from the subject of the record when possible. Third parties may be asked when information must be verified, opinions or evaluations are required, the subject cannot be contacted, or the subject requests the information be obtained from another person.

3.3.4. Give a PA Statement (PAS) orally or in writing to anyone from whom personal information is collected for a system of records, and whenever an individual's Social Security Number is requested. *(NOTE: Do this regardless of how you collect or record the answers. You may display a sign in areas where people routinely furnish this kind of information. Give a copy of the PAS if asked; however, do not ask the person to sign the PAS.)* A PAS must include the following four items: (See Attachment 2 for sample PAS.)

3.3.4.1. Authority: The legal authority is the United States Code or Executive Order authorizing the program the system supports.

3.3.4.2. Purpose: The reason the information is collected.

3.3.4.3. Routine Uses: A list of where and why the information will be disclosed outside DOD.

3.3.4.4. Disclosure: Voluntary or Mandatory. Use Mandatory only when disclosure is required by law and the individual will be penalized for not providing information. Include any consequences of nondisclosure in nonthreatening language.

3.3.5. Do not disclose an individual's Social Security Number (SSN) without an official need to know, this includes disclosing to personnel in USTRANSCOM and DOD-wide. Outside the DOD, SSN is not releasable under the DOD Privacy Act Program without the individual's consent, unless authorized under one of the 12 exceptions to the "No Disclosure Without Consent" Rule (DOD 5400.11-R, Privacy Program). An SSN is a personal identifier and will be protected as For Official Use Only (FOUO) (Executive Order 9397, 22 November 1943, Numbering System for Federal Accounts Relating to Individual Persons). *NOTE: This order is not adequate authority to collect a SSN to create a record.* When law does not require disclosing the SSN, or when the system of records was created after 1 January 1975, the SSN may be requested; however, the individual may deny disclosure, then use alternative means of identifying records. Military Services use the SSN as a Service number to reference the individual's official records. When requesting a SSN as identification to retrieve an existing record, do not restate this information. When requesting a SSN to create a record, advise the individual the statute, regulation, or rule authorizing the request and use for the SSN, and if the individual is legally

obligated to disclose. Do not deny anyone a legal right, benefit, or privilege for refusing to give their SSN unless the law requires disclosure, or a law or regulation adopted before 1 January 1975 requires the SSN and the Service uses it to verify a person's identity in a system of records established before that date.

3.3.6. Medical Information. Service element commanders, directors, CSG chiefs, functional managers, and supervisors within USTRANSCOM, where appropriate, are responsible for ensuring that the handling and release of protected healthcare information are in accordance with DOD 6025.18-R, DOD Health Information Policy Regulation.

4. DENIAL AUTHORITIES. The USTRANSCOM Commander (TCCC) and his designee, the Chief of Staff (TCCS) are the USTRANSCOM Privacy Act denial authorities. Access denials are processed within 5 workdays from receipt of the request for access. The System Manager for the information requested will prepare the "Recommendation for Access Denial" package to include a copy of the request, the record requested, and applicable exemption. Coordinate access denial recommendations through the Command Privacy Act Officer (TCCS-IMR). TCCS-IMR will review the proposed denial and coordinate through the Chief Counsel (TCJA) and Public Affairs (TCPA) for signature by the command denial authority (TCCC or TCCS). Notification of denials to requesters will include statutory authority, reason, and pertinent appeal rights. Before denying access to a record, ensure the system has an exemption approved by Air Force Chief Information Officer, Privacy (AF-CIO/P) or published as a final rule in the Federal Register; the exemption covers each document (all parts of a system are not automatically exempt); and nonexempt parts are segregated.

4.1. Medical Records. If a physician believes that disclosing requested medical records could harm the person's mental or physical health, ask the requester to get a letter from a physician to whom you can send the records and include a letter explaining that giving the records directly to the requester could be harmful. If naming a physician poses a hardship, offer the services of military physician other than the one who provided treatment; however, the requester is entitled to receive their records.

4.2. Third Party Information. Normally, when information in a requester's record is "about" or "pertains to" a third party, it is not considered the requester's record and should not be released. This is not considered a denial. However, if the requester will be denied a right, privilege, or benefit, the requester must be given access to relevant portions. If nonjudicial punishment or loss of privileges is the issue, appropriate portions will not be protected and will be released.

4.3. Civil Action Information. Records compiled in connection with a civil action or other proceeding, including any action where USTRANSCOM expects judicial or administrative adjudicatory proceedings, will not be released. This exemption does not include criminal actions. Attorney work products prepared before, during, or after the action or proceeding will not be released.

5. REQUESTING ACCESS TO PRIVACY ACT RECORDS. USTRANSCOM members or their designated representatives may request a copy of their records in a system of records. Requesters need not state why they want access to their records. Verify the identity of the requester to avoid unauthorized disclosures. How identity is verified will depend on the sensitivity of the requested record. A request from an individual for his or her own records in a system of records will be considered under both the Freedom of Information Act (FOIA) and PA regardless of the Act cited; however, there is no requirement to cite either Act if the records they want are contained in a system of records. Process the request under whichever Act gives the most information. Requesters should describe the records they want, with at least a type of record or functional area if they do not have the system of records number. For "all records about me" requests, refer the requester to www.defenselink.mil/privacy/notices to review Systems of Records published in the Federal Register. Requesters should not use government equipment, supplies, stationery, postage, telephones, or official mail channels for making PA requests. If records exist, inform the requester how to review the record. If possible, respond to PA requests within 10 workdays of receipt, or send a letter explaining why the request cannot be responded to within 10 workdays and give an approximate completion date no more than 20 workdays. Requester should be shown or given a copy of the record within 30 workdays unless the system is exempt (see Paragraph 12). If the system is exempt provide any parts releasable under FOIA, with appeal rights, citing appropriate exemptions from the PA and FOIA. If the requester wants another person present during the records review, the system manager may ask for written consent to authorize discussing the record with another person present. Give the first 100 pages free and charge only reproduction costs for the remainder at $.15 per page. Do not charge fees when the requester can get the record without charge under another publication, for search, for reproducing a document for the convenience of the command, or for reproducing a record so the requester can review it.

6. AMENDING THE RECORD:

6.1. Individuals may ask to have their records amended to make them accurate, timely, relevant, or complete. Systems managers routinely correct a record if the requester can show that it is factually wrong. Anyone may request minor corrections orally. Requests for more serious modifications should be in writing. After verifying the identity of the requester, make the change, notify all known recipients of the record, and inform the individual. Acknowledge requests for amendment within 10 workdays of receipt. Give an expected completion date unless the change is completed within that time. Final decisions must take no longer than 30 workdays.

6.2. USTRANSCOM will not usually amend a record when the change is based on opinion, interpretation, or subjective official judgment. This action constitutes a denial, and requesters may appeal. If the system manager decides not to amend or partially amend the record, send a copy of the request, the record, and the recommended denial reasons to the command PA officer, who will review the proposed denial and coordinate through TCJA and TCPA for signature by the command denial authority, TCCC or TCCS. If the denial authority approves the request,

amend the record and notify all previous recipients that it has been changed. Denial notification to requesters will include the statutory authority, reason, and pertinent appeal rights.

6.3. Requesters should pursue record corrections of subjective matters and opinions through proper channels to the Civilian Personnel Flight (CPF) using grievance procedures or the specific Service Board for Correction of Military Records. Record correction requests denied by CPF or Service Board for Correction of Military Records are not subject to further consideration under this instruction.

7. APPEAL PROCEDURES: Individuals may request a denial review within 60 calendar days after receiving a denial letter. The command Privacy Act Officer will complete the appeal package to include the original appeal letter, the initial request, the initial denial, a copy of the record, any internal records or coordination actions relating to the denial, denial authority comments on the appellant's arguments, and legal reviews, if applicable, and forward to AF-CIO/P, 1155 Air Force Pentagon, Washington, D.C. 20330-1155 through TCJA and TCPA for signature by the command denial authority, TCCC or TCCS. If the denial authority reverses an earlier denial and grants access or amendment, notify the requester immediately.

8. PRIVACY ACT NOTIFICATIONS:

8.1. USTRANSCOM will include a Privacy Act Warning Statement in each USTRANSCOM publication that requires collecting or keeping personal information in a system of records. Also include the warning statement when publications direct collection of SSN from individuals. The warning statement will cite legal authority and the system of records number and title. You can use the following warning statement: "This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by (United States Code citation and or Executive Order number). System of Records Notice (number and title) applies."

8.2. Information systems that contain information on individuals that is retrieved by name or personal identifier are subject to the Privacy Act. These systems are required to have a Privacy Act system notice published in the Federal Register that covers the information collection. In addition, all information systems subject to the Privacy Act will have warning banners displayed on the first screen (at a minimum) to assist in safeguarding the information. Use the following: **"***PRIVACY ACT INFORMATION – The information accessed through this system is FOR OFFICIAL USE ONLY and must be protected in accordance with the Privacy Act and USTRANSCOM Instruction 33-35."*

8.3. Exercise caution before transmitting personal information over electronic mail (e-mail) to ensure it is adequately safeguarded. Some information may be so sensitive and personal that e-mail may not be the proper way to transmit it. When sending personal information over e-mail within USTRANSCOM/DOD, ensure there is an official need; all addressees, including "cc" addressees, are authorized to receive it under the Privacy Act; and it is protected from

unauthorized disclosure, loss, or alteration. Protection methods may include encryption or password protecting the information. When transmitting personal information over e-mail, add "FOUO" to the beginning of the subject line, followed by the subject, and the following statement at the beginning of the e-mail (do not apply to bottom of e-mails): *"This e-mail contains FOR OFFICIAL USE ONLY (FOUO) information which must be protected under the Privacy Act and USTRANSCOMI 33-35."*

9. PRIVACY IMPACT ASSESSMENTS. The Electronic Government (E-Government) Act of 2002 requires a Privacy Impact Assessment (PIA) be conducted before developing or procuring information technology or initiating a new collection of information using information technology that collects, maintains, or disseminates information that permits identification of an individual. This includes online contact with a specific individual, if identical questions are posed to, or identical reporting requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the Federal Government. The PIA addresses what information is to be collected, why the information is being collected, the intended use of the information, with whom the information will be shared, what notice or opportunities for consent will be provided and how that information will be shared, secured, and whether a system of records is being created. The system manager will conduct a PIA as outlined in Attachment 3 and send it to the command Privacy Act Officer (TCCS-IMR) for review and to the command Chief Information Officer (CIO), Director, Command, Control, Communications and Computer Systems (TCJ6) for coordination. TCJ6 will send coordinated PIAs they recommend for approval to Air Force CIO for final decision through AF-CIO/P, 1155 Air Force Pentagon, Washington DC 20330-1155, or e-mail af.foia@pentagon.af.mil. Whenever practicable, approved PIAs will be posted to the FOIA/Privacy web site for public access at http://www.foia.af.mil (this requirement will be waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment). Additionally, the Office of Management and Budget (OMB) requires copies of PIAs for each system for which funding is requested.

10. PREPARING AND PUBLISHING SYSTEM NOTICES FOR THE FEDERAL REGISTER. USTRANSCOM must publish notices in the Federal Register of new, changed, and deleted systems to inform the public of the records USTRANSCOM keeps and give them an opportunity to comment. The Privacy Act also requires submitting new or significantly changed systems to OMB and both houses of the Congress before publication in the Federal Register. This includes starting a new system, instituting significant changes to an existing system, sending out data collection forms or instructions, and issuing a request for proposal or invitation for bid to support a new system. At least 120 days before implementing a new system of records, system managers must send a proposed system notice through TCCS-IMR to AF-CIO/P following the format in Attachment 4. TCCS-IMR will send notices electronically to af.foia@pentagon.af.mil using Microsoft Word and using the Track Changes tool in Word to indicate additions/changes to existing notices. On new systems of records, system managers must include a statement that a risk assessment was accomplished and is available should OMB request it. System managers

will review and validate their Privacy Act system notices annually and submit changes to TCCS-IMR for processing.

11. PROTECTING AND DISPOSING OF RECORDS:

11.1. When the system becomes operational, the system manager will establish appropriate safeguards to ensure the records are secure, confidential, and protected against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. The system manager will be responsible for data retained in the system of records, ensuring information maintained is current, and security procedures are complied with.

11.2. Information will be protected according to its sensitivity level. Consider the personal sensitivity of the information and the risk of loss or alteration. Most information in systems of records is FOUO. Contact TCFP for protection methods of FOUO material. Use of AF Visual Aid 33-276 *(Air Force Privacy Label)* on file folders (affixed to the folder tab, next to the file folder label) is optional. Use floppy disks (affix to the floppy disk, not to the disk jacket); computer tapes (affix to the computer tape disk reel); hard disk drive (affix to disk drive housing); and CD-ROM (affix to jewel box) to protect Privacy Act material. The AF Form 3227, *Privacy Act Cover Sheet*, is used for protecting Privacy Act material such as letters, file folders, listings, etc.; handcarrying material to and from offices; and working with Privacy Act material at workstations.

11.3. Balance additional protection against risk and cost. For example, a password may be enough protection for an automated system with a log-on protocol. Classified computer systems or those with established audit and password systems are obviously less vulnerable than unprotected files or word processors in offices that are periodically empty.

11.4. A Privacy Act case file will include requests from and replies to individuals on whether a system has records about them; requests for access or amendment; approvals, denials, appeals, and final review actions; and coordination actions and related documents. Do not keep copies of disputed records in the Privacy Act case file. Use the file solely for statistics and to process requests. Do not use the case files to make any kind of determination about an individual. Document reasons for untimely responses.

11.5. Records must be transferred in a manner that prevents unauthorized disclosure of information contained in a system of records. Use sealed opaque envelopes to transfer Privacy Act material by mail. Use sealed opaque envelopes or affix a label over the string closure of Optional Form 65-B (holey-joe) to transfer inter-base and inter-office Privacy Act material. Do not transmit a record from a system of records orally (by telephone or otherwise) to anyone unless the disclosure is authorized under the Privacy Act and until the recipient's identity and need to know are fully verified. Store paper record material or electronic media (floppy disks, CD-ROM disks, computer tapes, etc.) in a lockable container (filing cabinet, desk, etc.), or in a

secured room at all times when not in use during working hours, and at all times during nonworking hours. Local Area Network (LAN) access of Privacy Act protected files will be password protected with a log-on protocol authorized by the respective system manager. Do not leave Privacy Act records unattended and exposed at any time unless the entire work area is fully secured from unauthorized persons. Annotate each page of a document containing Privacy Act material with the statement, *"Personal Data – Privacy Act of 1974 Applies."* (This includes correspondence containing SSNs.) Mark all rosters/listings, which contain personal information (home address, home telephone number, or SSN) *"For Official Use Only (FOUO)"* and add one of the following statements:

11.5.1. Official, used for alert, recall, emergency notification, etc.: *"This (roster/listing) contains personal information and is to be used for official purposes only."*

11.5.2. Unofficial, used for social, special events planning: *"This (roster/listing) contains personal information and is to be used for social or quasi-social, special events planning purposes. Written consent has been secured from each individual listed."*

11.6. Within USTRANSCOM, destroy Privacy Act material by tearing into small pieces, shredding, or chemical decomposition to render material unrecognizable or beyond reconstruction. The destroyed material may then be placed in trash containers. USTRANSCOM *will not use recycling* as a method of destroying Privacy Act material. Clear magnetic tapes or other magnetic medium by degaussing, overwriting, or erasing. It is the system manager's responsibility to ensure this process is accomplished.

12. PRIVACY ACT EXEMPTIONS. A system manager who believes that a system of records needs an exemption from some or all of the requirements of the Privacy Act should send a request to AF-CIO/P through the TCCS-IMR. The request should detail the reasons for the exemption, the section of the Act that allows the exemption, and specific subsections of the Privacy Act from which the system is to be exempted, with justification for each subsection. Denial authorities can withhold records using these exemptions only if they were previously approved and published as an exemption for the system in the Federal Register. Exemption types include:

12.1. General exemptions free a system from most parts of the Privacy Act.

12.2. Specific exemptions free a system from only a few parts.

12.3. Approved exemptions exist under 5 United States Code 552a for:

12.3.1. Certain systems of records used by activities whose principal function is criminal law enforcement (subsection [j][2]) The following Air Force Systems of Records are exempt under 5 United States code (U.S.C.) Section 552a [j] [2]:

12.3.1.1. F031 AF SP A, Correction and Rehabilitation Records (parts may be exempt).

12.3.1.2. F031 AF SP E, Security Forces Management Information System (parts may be exempt).

12.3.1.3. F051 AF JA F, Courts-Martial and Article 15 Records (parts may be exempt).

12.3.1.4. F071 AF OSI A, Counter Intelligence Operations and Collection Records.

12.3.1.5. F071 AF OSI C, Criminal Records.

12.3.1.6. F071 AF OSI D, Investigative Support Records.

12.3.1.7. F090 AF IG B, Inspector General Records (parts may be exempt).

12.3.2. Classified information in any system of records (subsection [k][1]).

12.3.3. Law enforcement records (other than those covered by subsection [j][2]). The Air Force must allow an individual access to any record issued to deny rights, privileges or benefits to which he or she would otherwise be entitled by federal law or for which he or she would otherwise be eligible as a result of the maintenance of the information (unless doing so would reveal a confidential source) (subsection [k][2]). The following Air Force Systems of Records are exempt under 5 U.S.C. Section 552a [k] [2]:

12.3.3.1. F 031 497IG A, Sensitive Compartmental Information Personnel Records.

12.3.3.2. F 036 AF DPG, Military Equal Opportunity and Treatment (parts may be exempt).

12.3.3.3. F 044 AF SG Q, Family Advocacy Program Records (parts may be exempt).

12.3.3.4. F 051 AF JA F, Courts-Martial and Article 15 Records (parts may be exempt).

12.3.3.5. F 051 AF JA I, Commander Directed Inquiries (parts may be exempt).

12.3.4. Statistical records required by law. Data is for statistical use only and may not be used to decide individuals' rights, benefits, or entitlements (subsection [k][4]).

12.3.5. Data to determine suitability, eligibility, or qualifications for federal service or contracts, or access to classified information if access would reveal a confidential source (subsection [k][5]). The following Air Force Systems of Records are exempt under 5 U.S.C Section 552a [k] [5]:

12.3.5.1. F 031 DOD A, Joint Personnel Adjudication Systems (parts may be exempt).

12.3.5.2. F 031 497IG A, Sensitive Compartmental Information Personnel Records.

12.3.5.3. F 031 497IG B, Special Security Case Files.

12.3.5.4. F 031 AF SP N, Special Security Files.

12.3.5.5. F 036 AF PC P, Applications for Appointment and Extended Active Duty Files (parts may be exempt).

12.3.5.6. F 036 AETC I, Cadet Records (parts may be exempt).

12.3.5.7. F 044 AF SG Q, Family Advocacy Program Records (parts may be exempt).

12.3.5.8. F 071 AF OSI B, Security and Related Investigative Records.

12.3.5.9. F 071 AF OSI F, Investigative Applicant Processing Records.

12.3.6. Qualification tests for appointment or promotion in the Federal service if access to this information would compromise the objectivity of the tests (subsection [k][6]). The following Air Force Systems of Records are exempt under 5 U.S.C. Section 552a [k] [6]:

12.3.6.1. F 036 AFPC K, Historical Airman Promotion Master Test File.

12.3.6.2. F 036 AFPC N, Air Force Personnel Test 851, Test Answer Sheets.

12.3.7. Information, which the Armed Forces uses to evaluate potential for promotion if access to this information would reveal a confidential source (subsection [k][7]). The following Air Force Systems of Records are exempt under 5 U.S.C. Section 552a [k] [7]:

12.3.7.1. F 036 AF DP A, files on general officers and colonels assigned to general officer positions.

12.3.7.2. F 036 AF PC A, Effectiveness/Performance Reporting System (parts may be exempt).

12.3.7.3. F 036 AF PC O, General Officer Personnel Data System (parts may be exempt).

12.3.7.4. F 036 USAFA A, Cadet Personnel Management System (parts may be exempt).

12.3.7.5. F 036 USAFA B, Master Cadet Personnel Record (parts may be exempt).

12.3.7.6. F 036 USAFA K, Admissions Records (parts may be exempt).

13. DISCLOSING RECORDS TO THIRD PARTIES:

13.1. Before releasing personal information to third parties, consider the consequences, check accuracy, and make sure that no law or directive bans disclosure. Personal information can be released to third parties when the subject agrees orally or in writing. USTRANSCOM staff members consent to releasing their home telephone number and address when they sign and check the "Consent" block on the Individual Personnel Data Report maintained by the Manpower and Personnel Directorate (TCJ1). Before including personal information such as home addresses, home phones, and similar information on social rosters or directories, ask for written consent statements. Otherwise, do not include the information.

13.2. You must get written consent before releasing a SSN, marital status, number and sex of dependents, race, gross salary of military personnel (see paragraph 13.3. for releasable pay information), civilian educational degrees and major areas of study (unless the request for information relates to the professional qualification for federal employment), school and year of graduation, home of record, home address and phone number, age and date of birth, present or future assignments for overseas or for routinely deployable or sensitive units, and office and unit address and duty phone for overseas or for routinely deployable or sensitive units. *(Note: These are not all inclusive.)*

13.3. Consent is not required to release name, rank, and grade; service specialty codes; pay (including base pay, special pay, and all allowances except Basic Allowance for Housing); gross salary for civilians; past duty assignments; present and future approved and announced stateside assignments; position title, office, unit address, and duty phone number; date of rank; date entered on active duty; pay date; source of commission; professional military education; promotion sequence number; military awards and decorations; duty status of active, retired, or reserve; active duty official attendance at technical, scientific, or professional meetings; biographies and photos of key personnel; and date of retirement/separation.

13.4. Information that can be obtained by authorized individuals for official purposes on a need to know basis from existing systems of records in USTRANSCOM include:

13.4.1. Miscellaneous personnel management actions (alert or recall rosters; wartime, mobility, emergency actions or assignments; shelter duties or assignments, etc.); off-duty employment information; and *ON A VOLUNTARY PROVIDED BASIS ONLY*, an individual's involvement in off-duty activities for rendering performance/evaluation reports.

13.4.2. Dependent (spouse and children) information (name, age, sex, nationality, home address, home telephone number, etc., and special needs such as availability of special education or

treatment facilities. (*NOTE: Dependent information used for unofficial or quasi-official use will be ON A VOLUNTARILY PROVIDED BASIS ONLY.)*

13.5. Information for social rosters (name, address, phone number, official title or position; invitations, acceptance, regrets, protocol) to include dependent information will be obtained *ON A VOLUNTARILY PROVIDED BASES ONLY.*

13.6. Information for special events planning (biographical data including, but not limited to: name, duty, and home address) telephone numbers; name of spouse and family; description of position in business and community affiliations with military-oriented civic organizations; and photos will be *ON A VOLUNTARILY PROVIDED BASIS ONLY*.

13.7. When disclosing other information, consider if the subject would have a reasonable expectation of privacy in the information requested, and would disclosing the information benefit the general public? USTRANSCOM considers information as meeting the public interest standard if it reveals anything regarding the operations or activities of the agency, or performance of its statutory duties. Balance the public interest against the individual's probable loss of privacy. Do not consider the requester's purpose, circumstances, or proposed use.

13.8. USTRANSCOM may release information without consent to:

13.8.1. Respond to FOIA requests when information is releasable.

13.8.2. Officials or employees within DOD with a need to know.

13.8.3. Agencies outside DOD for a routine use published in the Federal Register. The purpose of the disclosure must be compatible with the purpose in the routine use. When initially collecting the information from the subject, the “Routine Uses” block in the Privacy Act Statement must name the agencies and reason.

13.8.4. The Bureau of the Census to plan or carry out a census or survey under Title 13, United States Code, Section 8.

13.8.5. A recipient for statistical research or reporting. The recipient must give advanced written assurance that the information is for statistical purposes only. (*NOTE: No one may use any part of the record to decide an individuals' rights, benefits, or entitlements. You must release records in a format that makes it impossible to identify the real subjects.)*

13.8.6. The Archivist of the United States and the National Archives and Records Administration to evaluate records for permanent retention.

13.8.7. A federal, state, or local agency (other than DOD) for civil or criminal law enforcement. TCCC or his designee, TCCS, must send a written request to the system manager specifying the record or part needed and the law enforcement purpose. The system manager may also disclose a record to a law enforcement agency if the agency suspects a criminal violation. This disclosure is a routine use for all DOD systems of records and is published in the Federal Register.

13.8.8. An individual or agency that needs the information for compelling health or safety reasons. The affected individual need not be the record subject.

13.8.9. Congress, a congressional committee, or a subcommittee, for matters within their jurisdictions.

13.8.10. A congressional office acting for the record subject. A published, blanket routine use permits this disclosure. If the material for release is sensitive, obtain a release statement first.

13.8.11. The Comptroller General or an authorized representative of the General Accounting Office on business.

13.8.12. A court order of a court of competent jurisdiction, signed by a judge.

13.8.13. A consumer credit agency according to the Debt Collections Act when a published system notice lists this disclosure as a routine use.

13.9. Service personnel may disclose the medical records of minors to their parents or legal guardians. The laws of each state define the age of majority. Services must obey state laws protecting medical records of drug or alcohol abuse treatment, abortion, and birth control. Outside the United States (overseas), the age of majority is 18. Unless parents or guardians have a court order granting access or the minor's written consent, they will not have access to minor's medical records overseas when the minor sought or consented to treatment between the ages of 15 and 17 in a program where regulation or statute provides confidentiality of records and he or she asked for confidentiality.

13.10. Systems managers must keep an accurate record of all disclosures made from any system of records except disclosures to DOD personnel for official use or disclosures under the FOIA. Use Air Force Form 771, *Accounting of Disclosures*, for record disclosure tracking. *(NOTE: Disclosure of personal records to a contractor for use in the performance of a USTRANSCOM contract is considered a disclosure within the agency.)*

14. COMPUTER MATCHING PROGRAMS. Computer matching programs electronically compare records from two or more automated systems that may include DOD, another Federal agency, or a state or other local government. Proposed matches that could result in an adverse action against a Federal employee must meet the following requirements: a written agreement

between participants, approval of the Defense Data Integrity Board, matching notice published in Federal Register before matching begins, full investigation and due process enforced, and act on the information, as necessary. The Privacy Act applies to matching programs that use records from Federal personnel or payroll systems and Federal benefit programs where matching determines Federal benefit eligibility, checks on compliance with benefit program requirements, recovers improper payments or delinquent debts from current or former beneficiaries. Matches used for statistics, pilot programs, law enforcement, tax administration, routine administration, background checks and foreign counterintelligence, and internal matching that will not cause any adverse action are exempt from the Privacy Act matching requirements. Contact TCCS-IMR before participating in a matching program. *(NOTE: Allow 180 days for processing requests for a new matching program.)*

15. PRIVACY AND THE WEB. *Do not* post personal information on publicly accessible DOD web sites unless clearly authorized by law and implementing regulation and policy. Additionally, *do not* post personal information on non-publicly accessible web sites unless it is mission essential and appropriate safeguards have been established. Public web sites will comply with privacy policies regarding restrictions on persistent and third party cookies, and appropriate privacy and security notices at major web site entry points will be added as well as Privacy Act statements or Privacy Advisories when collecting personal information. A Privacy Act Statement will be included on the web page that collects information directly from an individual, and that information is maintained and retrieved by an individual's personal identifier (i.e., SSN). Personal information will be maintained only in approved Privacy Act systems of records that are published in the Federal Register. Anytime a web site solicits personally-identifying information, even when not maintained in a Privacy Act system of records, it requires a Privacy Advisory, which informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the web page where the information is being solicited, or through a well-marked hyperlink *"Privacy Advisory – Please refer to the Privacy and Security Notice that describes why this information is collected and how it will be used."*

16. TRAINING. The Privacy Act requires training for all persons involved in the design, development, operation and maintenance of any system of records. More specialized training is needed for personnel who may be expected to deal with the news media or the public, personnel specialists, finance officers, information managers, supervisors, and individuals working with medical and security records. The above personnel are required to have annual training in the principles and requirements of the Privacy Act. USTRANSCOM training aids include USTRANSCOM Pamphlet 33-40, The Privacy Act Program - A Manager's Overview, the Air Force FOIA web page at www.foia.af.mil, and the annual Freedom of Information Act and Privacy Act training at USTRANSCOM, on-site.

17. INFORMATION COLLECTIONS, RECORDS, AND FORMS OR INFORMATION MANAGEMENT TOOLS.

17.1. No information collections are required by this publication.

17.2. Retain and dispose of Privacy Act records according to CJCSM 5760.01, Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures, and Volume II, Disposition Schedule.

\\SIGNED\\
MARY E. WILSON
Chief, Information Management

Attachments
1. Glossary of References, Abbreviations, Acronyms, and Terms
2. Sample PAS
3. Privacy Impact Assessment
4. Procedures for Preparing a Privacy Act System Notice

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

Section A - References

Executive Order 9397, 22 November 1943, Numbering System for Federal Accounts Relating to Individual Persons

32 Code of Federal Regulations 806b-13, Air Force Privacy Act Program

Title 5, United States Code, Section 552, The Freedom of Information Act

Title 5, United States Code, Section 552a, as amended, The Privacy Act of 1974

Title 10 United States Code, Section 164, Armed Forces, Organization and General Military Powers, Combatant commands

Title 10 United States Code, Section 3013, Armed Forces Organization, Department of the Army

Title 10 United States Code, Section 5013, Armed Forces Organization, Department of the Navy

Title 10 United States Code, Section 8013, Armed Forces Organization, Department of the Air Force

Title 13 United States Code, Section 8, Census, Administration, General Provisions

Public Law 100-235, The Computer Security Act of 1987

Public Law 100-503, The Computer Matching and Privacy Act of 1988

Public Law 104-13, Paperwork Reduction Act of 1995

Public Law 107-347, Section 208, Electronic Government Act of 2002

Federal Register

Chairman Joint Chiefs of Staff Manual 5760.01, Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures and Volume II, Disposition Schedule

Department of Defense Regulation 6025.18, DOD Health Information Policy Regulation

Department of Defense Directive 5400.11, Department of Defense Privacy Program

Department of Defense Regulation 5400.11, Department of Defense Privacy Program

Air Force Instruction 33-332, Air Force Privacy Act Program

Section B - Abbreviations and Acronyms

AF	Air Force
AF-CIO-P	Air Force Chief Information Officer - Privacy
DOD	Department of Defense
CIO	Chief Information Officer
CJCSM	Chairman Joint Chiefs of Staff Manual
CPF	Civilian Personnel Flight
E-Government	Electronic Government
E-Mail	Electronic Mail
FOIA	Freedom of Information Act
FOUO	For Official Use Only
OMB	Office of Management and Budget
PAS	Privacy Act Statement
PIA	Privacy Impact Assessment
SSN	Social Security Number
TCCC	USTRANSCOM Commander
TCCS	USTRANSCOM Chief of Staff
TCCS-IM	USTRANSCOM Chief of Staff, Information Management
TCCS-IMR	USTRANSCOM Chief of Staff, Information Management, Information Management Communications and Records Management
TCFP	USTRANSCOM Force Protection
TCJA	USTRANSCOM Chief Counsel
TCJ1	USTRANSCOM Manpower and Personnel Directorate
TCJ6	USTRANSCOM Command, Control, Communications and Computer Systems Directorate
TCPA	USTRANSCOM Public Affairs
USTRANSCOM	United States Transportation Command

Section C – Terms

Access. Allowing individuals to review or receive copies of their records.

Agency. For the purposes of disclosing records subject to the Privacy Act among Department of Defense (DOD) Components, the DOD is considered a single agency. For all other purposes to include applications for access and amendment, denial of access or amendment, appeals from denials, and recordkeeping as regards release to non-DOD agencies; each DOD Component is considered an agency within the meaning of the Privacy Act.

Amendment. The process of adding, deleting, or changing information in a system of records to make the data accurate, relevant, timely, or complete.

Computer Matching. A computerized comparison of two or more automated systems of records or a system of records with non-Federal records to establish or verify eligibility for payments under Federal benefit programs or to recover delinquent debts for these programs.

Confidential Source. A person or organization who has furnished information to the Federal Government under an express promise that the person's or the organization's identity will not be disclosed or under an implied promise of such confidentiality if this implied promise was made before 27 September 1975.

Confidentiality. An expressed and recorded promise to withhold the identity of a source or the information provided by a source. The Air Force promises confidentiality only when the information goes into a system with an approved exemption for protecting the identify of confidential sources.

Denial Authority. The individuals with authority to deny requests for access or amendment of records under the Privacy Act.

Disclosure. The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government agency, other than the subject of the record, the subject's designated agent, or the subject's legal guardian.

Individual. A living citizen of the United States or an alien lawfully admitted to the United States for permanent residence. The legal guardian of an individual has the same rights as the individual and may act on his or her behalf. No rights are vested in the representative of a dead person under this instruction and the term "individual" does not embrace an individual acting in an interpersonal capacity (for example, sole proprietorship or partnership).

Individual Access. To make available information pertaining to the individual by the individual or his or her designated agent or legal guardian.

Maintain. Includes collecting, safeguarding, using, accessing, amending, and disseminating personal information.

Matching Agency. The agency that performs a computer match.

Member of the Public. Any individual or party acting in a private capacity to include Federal employees or military personnel.

Minor. Anyone under the age of majority according to local state law. If there is no applicable state law, a minor is anyone under age 18. Military members and married persons are not minors, no matter what their chronological age.

Official Use. Within the context of this instruction, this term is used when employees of a DOD component have a demonstrated need for the use of any records or the information contained therein in the performance of their authorized duties.

Personal Identifier. A name, number, or symbol which is unique to an individual, usually the person's name or Social Security Number (SSN).

Personal Information. Knowledge about an individual that is intimate or private to the individual, as distinguished from that related solely to the individual's official functions or public life.

Privacy Act Request. A request from an individual for notification as to the existence of, access to, or amendment of records pertaining to that individual. These records must be maintained in a system of records.

Privacy Act Statement (PAS). A statement furnished to an individual when the individual is requested to provide personal information, regardless of the medium used to collect the information, to go into a system of records. A PAS is also furnished to an individual when asking them for their SSN.

Privacy Impact Assessment (PIA). A written assessment of an information system that addresses the information to be collected, the purpose and intended use; with whom the information will be shared; notice or opportunities for consent to individuals; how the information will be secured; and whether a new system of records is being created under the Privacy Act.

Record. Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Routine Use. The disclosure of a record outside the DOD for a use that is compatible with the purpose for which the information was collected and maintained by the DOD. The routine use must be included in the published system notice for the system of records involved. For example: "To the Veterans Administration to verify the physical disability of applicants for the purpose of authorizing monthly retirement disability payments."

Source Agency. A federal, state, or local government agency that discloses records for the purpose of a computer match.

System Manager. The individual who initiates a system of records, operates such system, or is responsible for a segment of a decentralized part of that system and issues policies and procedures for operating and safeguarding of information in the system.

System Notice. The official public notice published in the Federal Register of the existence and content of the system of records.

System of Records. A group of records under the control of a DOD component from which information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to the individual and published in the Federal Register.

SAMPLE PRIVACY ACT STATEMENT

JOINT PERSONNEL SYSTEM

AUTHORITY: Title 5 United States Code, Section 301; Title 10 United States Code, Sections 164, 3013, 5013, and 8013; Executive Order 9397.

PURPOSES: To provide USTRANSCOM Commander, Deputy Commander, Chief of Staff, element commanders, directors, chiefs of direct reporting elements, functional managers, and supervisors: (1) A ready source of information for day-to-day operations and administrative determinations pertaining to assigned personnel, (2) A protocol listing to include spouses' names for social/special events planning. Use of the SSN is necessary for establishing a record and identification control in the automated system.

ROUTINE USES: Information will not be released outside of the Department of Defense.

DISCLOSURE: Voluntary: (1) The furnishing of civilian/military member information is voluntary; but failure to provide it may result in your not receiving/could hamper/could delay personnel support. (2) The furnishing of dependent information is voluntary.

PRIVACY IMPACT ASSESSMENT

Section A—Introduction and Overview

Privacy issues must be addressed when automated systems are being developed, and privacy protections must be integrated into the development life cycle of these automated systems. The vehicle for addressing privacy issues in a system under development is the Privacy Impact Assessment (PIA). The PIA process also provides a means to assure compliance with applicable laws and regulations governing individual privacy. The purpose of this document is to establish the requirements for addressing privacy during the systems development process, describe the steps required to complete a PIA, and define the privacy issues you will address in the PIA.

The United States Transportation Command (USTRANSCOM) is responsible for ensuring the privacy, confidentiality, integrity, and availability of personal information of all members, including civilian, military, and contract personnel. The USTRANSCOM Commander recognizes that privacy protection is both a personal and fundamental right. Among the most basic of individuals' rights is an expectation that the command will protect the confidentiality of personal, financial, and employment information. All command staff members also have the right to expect that the command will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out the command mission and responsibilities.

The USTRANSCOM Privacy Act Office, Information Management Communications and Records Management (TCCS-IMR) falls under responsibility of the Chief of Staff , Information Management (TCCS-IM). TCCS-IMR manages the command Privacy Act (PA) program.

Section B—Privacy and Systems Development

Rapid advancements in computer technology makes it possible to store and retrieve vast amounts of data of all kinds quickly and efficiently. These advancements have raised concerns about the impact of large computerized information systems on the privacy of data subjects. Public concerns about highly integrated information systems operated by the government make it imperative to commit to a positive and aggressive approach to protecting individual privacy. The USTRANSCOM Chief Information Officer, Director, Command, Control, Communications and Computer Systems (TCJ6) is requiring the use of this PIA in order to ensure that the systems the command develops protect individuals' privacy. The PIA incorporates privacy into the development life cycle so that all system development initiatives can appropriately consider privacy issues from the earliest stages of design.

The PIA is a process used to evaluate privacy in information systems. The process is designed to guide system owners and developers in assessing privacy through the early stages of development. The process consists of privacy training, gathering data from a project on privacy issues, and identifying and resolving the privacy risks. The PIA is initiated in the early stages of the development of a system and completed as part of the required system life cycle reviews. Privacy must be considered when requirements are being analyzed and decisions are being made

about data usage and system design. This applies to all of the development methodologies and system life cycles used in the command. Both the system owner and system developers must work together to complete the PIA. System owners must address what data is to be used, how the data is to be used, and who will use the data. The system developers must address whether the implementation of the owner's requirements presents any threats to privacy. Accomplish PIAs when developing or procuring information technology (IT) that collects, maintains, or disseminates information that permits identifying an individual; initiating a new collection of information, using IT, that collects, maintains, or disseminates information that permits identifying an individual, including online contacting of a specific individual, if identical questions are posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government; or systems as described above that are undergoing major modifications. TCCS-IMR reserves the right to request that a PIA be completed on any system that may have privacy risks.

Section C—Completing a Privacy Impact Assessment

The following steps are required to complete a PIA:

TCCS-IMR will provide training to the personnel responsible for writing the PIA document, describing the PIA process and providing details about the privacy issues and privacy questions to be answered to complete the PIA.

The system owner and developer will answer the privacy questions in Section E with a brief explanation for each questions. Issues that do not apply to a system should be noted as "Not Applicable." During the development of the PIA document, TCCS-IMR will be available to answer questions related to the PIA process and other concerns that may arise with respect to privacy.

The system owner will submit the completed PIA document to TCJ6, through TCCS-IMR, for review and recommendation to the Air Force Chief Information Officer-Privacy Office (AF-CIO/P).

The system life cycle review process (Command, Control, Communications, Computers, and Intelligence Support Plan) will be used to validate the incorporation of the design requirements to resolve the privacy risks. AF-CIO will issue final approval of the PIA.

Section D—Privacy Issues in Information Systems

Title 5, United States Code, 552a, The Privacy Act of 1974, as amended, requires Federal Agencies to protect personally identifiable information. It states specifically:

"Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President; collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and

privileges under Federal programs; maintain all records used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonable necessary to assure fairness to the individual in the determination; establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

To fulfill the commitment of USTRANSCOM to protect personal information, the following issues must be addressed with respect to privacy: The use of information must be controlled; information may be used only for a necessary and lawful purpose; individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them; information collected for a particular purpose would not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law; and any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual. Given the availability of vast amounts of stored information and the expanded capabilities of information systems to process information, it is foreseeable that there will be increased requests to share that information. With the potential expanded use of data in automated systems, it is important to remember that information can only be used for the purpose for which it was collected unless other uses are specifically authorized or mandated by law. If the data is to be used for other purposes, then the public must be provided notice of those other uses. These procedures do not in themselves create any legal rights, but are intended to express the full and sincere commitment of the command to protect individual privacy rights and which provide redress for violations of those rights.

The sources of the information in the system are an important privacy consideration if the data is gathered from other than USTRANSCOM records. Information collected from non-USTRANSCOM sources should be verified, to the extent practicable, for accuracy, that the information is current, and complete. This is especially important if the information will be used to make decisions about individuals.

Users of the data in a system can be individuals, other systems, and other agencies. Individuals who have access to the data can be system users, system administrators, system owners, managers, and developers. Users must be defined and documented and when they are granted access to a system, their access should be limited, where possible, to only that data needed to perform their assigned duties. If individuals are granted access to all of the data in a system, procedures need to be in place to deter and detect browsing and unauthorized access. Other systems are any programs or projects that interface with the system and have access to the data. Other agencies can be International, Federal, state, or local entities that have access to USTRANSCOM data.

Requirements for data to be used in the system must include the privacy attributes of the data, derived from the legal requirements imposed by The Privacy Act of 1974. The data must be relevant and necessary to accomplish the purpose of the system and must be complete, accurate, and timely. It is important to ensure the data has these privacy attributes in order to assure fairness to the individual in making decisions based on the data.

When administrative controls of automated systems are consolidated, they should be evaluated so that all necessary controls remain in place to continue to control access to and use of the data. Record retention procedures require review to ensure they meet statutory and/or information resources management requirements. Precise rules must be established for the length of time information is maintained and for assuring that it is properly disposed of at the end of that time.

Section E—Privacy Questions

Group I – Data in the System

1. Generally describe the information to be used in the system.

2. What are the sources of the information in the system?
   a. What USTRANSCOM files and databases are used?
   b. What Federal Agencies are providing data for use in the system?
   c. What State and local agencies are providing data for use in the system?
   d. What other third party sources will data be collected from?
   e. What information will be collected from the employee?

3. a. How will data collected from sources other than USTRANSCOM records and the subject be verified for accuracy?
   b. How will data be checked for completeness?
   c. Is the data current? How do you know?

4. Are the data elements described in detail and documented? If yes, what is the name of the document?

Group II – Access to the Data

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?

5. a. Do other systems share data or have access to data in this system? If yes, explain.
   b. Who will be responsible for protecting the privacy rights of the employees affected by the interface?

6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?
   b. How will the data be used by the agency?
   c. Who is responsible for assuring proper use of the data?
   d. How will the system ensure that agencies only get the information they are entitled to under applicable laws?

Group III – Attributes of the Data

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?
   b. Will the new data be placed in the individual's record?
   c. Can the system make determinations about the record subject that would not be possible without the new data?
   d. How will the new data be verified for relevance and accuracy?

3. a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
   b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.

   a. What are the potential effects on the due process rights of record subjects of consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies. How are the effects to be mitigated?

Section IV – Maintenance of Administrative Controls

1. a. Explain how the system and its use will ensure equitable treatment of record subjects.
   b. If the system is operated at more than one location, how will consistent use of the system and data be maintained?
   c. Explain any possibility of disparate treatment of individuals or groups.

2. a. What are the retention periods of data in this system?
   b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?
   c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

3. a. Is the system using technologies in ways that USTRANSCOM has not previously employed?
   b. How does the use of this technology affect personal privacy?

4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
   b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.
   c. What controls will be used to prevent unauthorized monitoring?

5. a. Under which Systems of Record notice does the system operate? Provide number and name.
   b. If the system is being modified, will the system of record require amendment or revision? Explain.

PROCEDURES FOR PREPARING A PRIVACY ACT SYSTEM NOTICE

The following elements comprise a system of records notice for publication in the Federal Register:

1. System identification (ID) number. The Air Force Chief Information Officer, Privacy Office (AF-CIO/P) assigns the notice number; for example, F044 AF TRANSCOM A, where "F" indicates "Air Force," the next number represents the records management disposition series, and the final letter group shows the system manager's command. The last character "A" indicates that this is the first notice for this series and system manager.

2. System name. Use a short, specific, plain-language title that identifies the system's general purpose, limited to 55 characters.

3. System location. Specify the address of the primary system and any decentralized elements, including automated data systems with a central computer facility and input or output terminals at separate locations. Use street address, 2-letter state abbreviations, and 9-digit ZIP codes. Spell out office names. Do not use office symbols.

4. Categories of individuals covered by the system. Use nontechnical, specific categories of individuals about whom USTRANSCOM keeps records. Do not use categories like "all USTRANSCOM personnel" unless they are actually true.

5. Categories of records in the system. Describe in clear, nontechnical terms the types of records maintained in the system. List only documents actually retained in the system of records. Do not show source documents that are used to collect data and then destroyed. Do not list form numbers.

6. Authority for maintenance of the system. Cite the specific law or Executive Order that authorizes the program the records support. Cite the Department of Defense (DOD) directive or instruction or other instruction that authorizes the system of records. Always include title with the citations. *NOTE: Executive Order 9397 authorizes using the SSN. Include this authority whenever the SSN is used to retrieve records.*

7. Purpose(s). Describe briefly and specifically what USTRANSCOM does with the information collected.

8. Routine uses of records maintained in the system, including categories of users, uses, and purposes of such uses. The blanket routine uses that appear at the beginning of each agency compilation in the Federal Register apply to all system notices unless the individual system notice specifically states that one or more of them do not apply to the system. Also, list each specific agency or activity outside DOD to whom the records may be released and the purpose for such release.

9. Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system.

9.1. Storage. Indicate the medium in which the records are maintained; i.e., file folders, card files, microfiche, computer, etc. Storage does not refer to the container or facility.

9.2. Retrievability. Specify how the records are retrieved; i.e., name and SSN, or personal characteristics (such as fingerprints or voiceprints).

9.3. Safeguards. List categories of agency personnel having immediate access and those responsible for safeguarding the records from unauthorized use. Identify system safeguards (safes, vaults, guards, etc.), but not in such detail as to compromise system security.

9.4. Retention and disposal. Disposal and accounting of records will be in accordance with Chairman Joint Chiefs of Staff Manual 5760.01, Joint Staff and Combatant Command Records Management Manual, Volume I, Procedures and Volume II, Disposition Schedule. When appropriate, also state length of time records are maintained by the agency, when they are transferred to a Federal Records Center, length of retention at the Records center, when they are transferred to the National Archives, or destroyed. State how records protected by the Privacy Act are destroyed: any method that prevents compromise, such as tearing, burning, or shredding, so long as the personal data is not recognizable and beyond reconstruction; degauss or overwrite magnetic tapes or other magnetic medium. Reference to an agency regulation without further detail is insufficient.

10. Systems manager(s) and address. List the title and duty address of the system manager. For decentralized systems, show the locations and the position or duty title of each category of officials responsible for any segment of the system.

11. Notification procedure. List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit; i.e., full name, military status, SSN, date of birth, or proof of identity, etc.

12. Record access procedures. Explain how individuals may arrange to access their records. Include the titles or categories of officials who may assist; i.e., the system manager.

13. Contesting records procedures. AF-CIO/P provides this standard caption.

14. Record source categories. Show categories of individuals or other information sources for the system. Do not list confidential sources protected by 5 United States Code, Section 552a, subsections (k)(2), (k)(5), or (k)(7) of the Privacy Act.

15. Exemptions claimed for the system. When a system has no approved exemption, write "none" under this heading. Specifically list any approved exemption including the subsection in the Privacy Act.